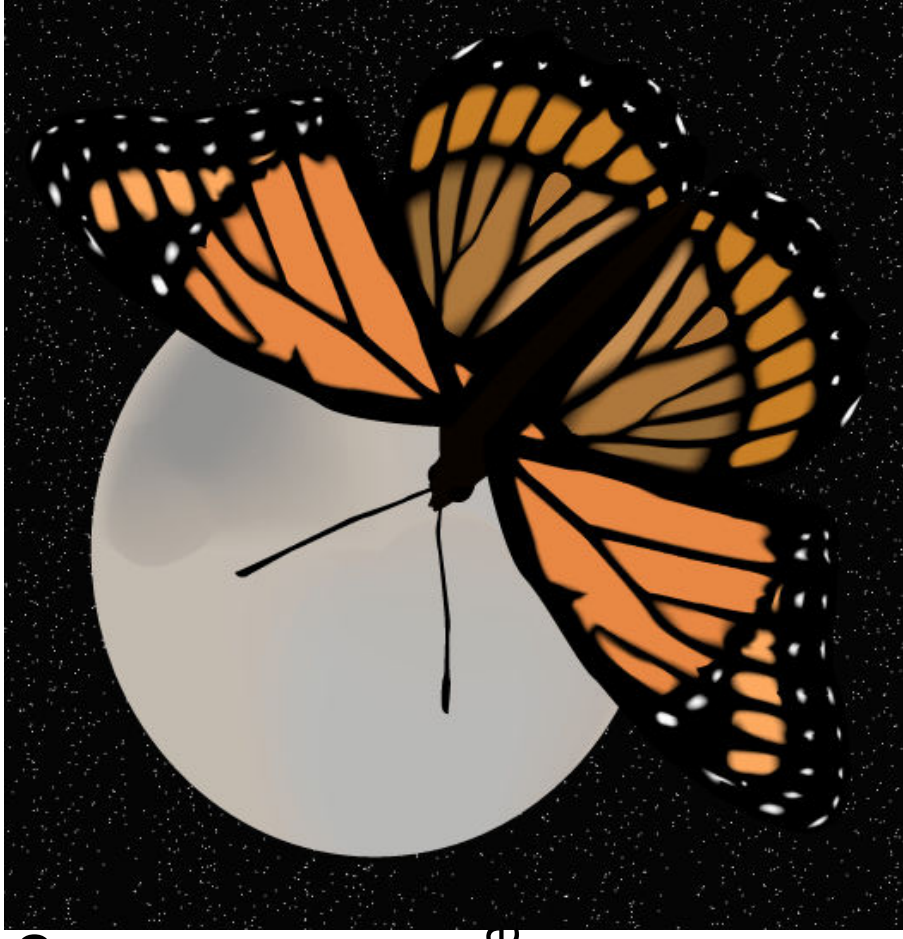


La conscience de l'environnement de l'entreprise: **"Situational Awareness"**

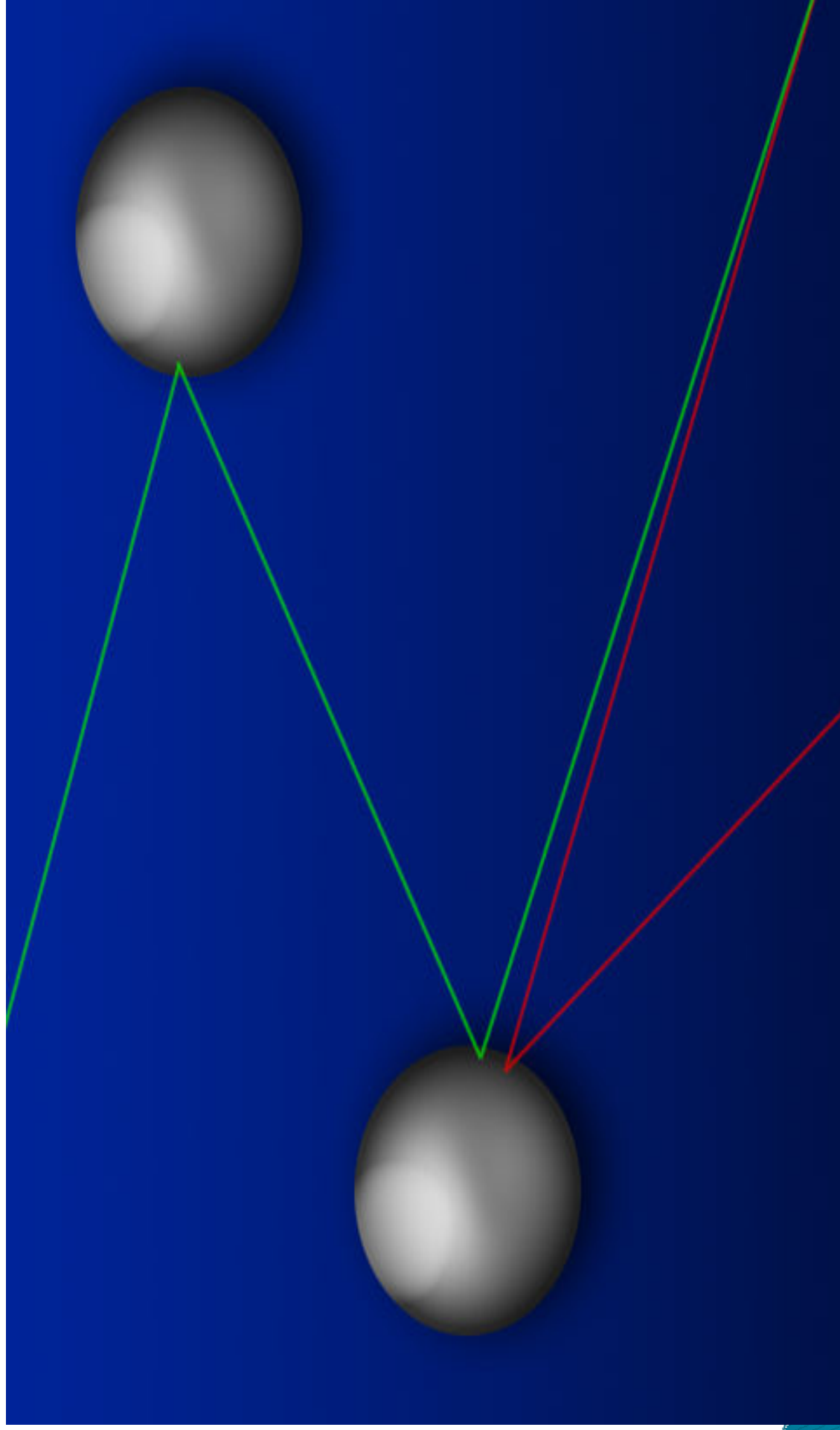
Général Mac Arthur : “Toutes les batailles perdues
se résument à deux mots : trop tard” .

L'univers de l'entreprise est en expansion

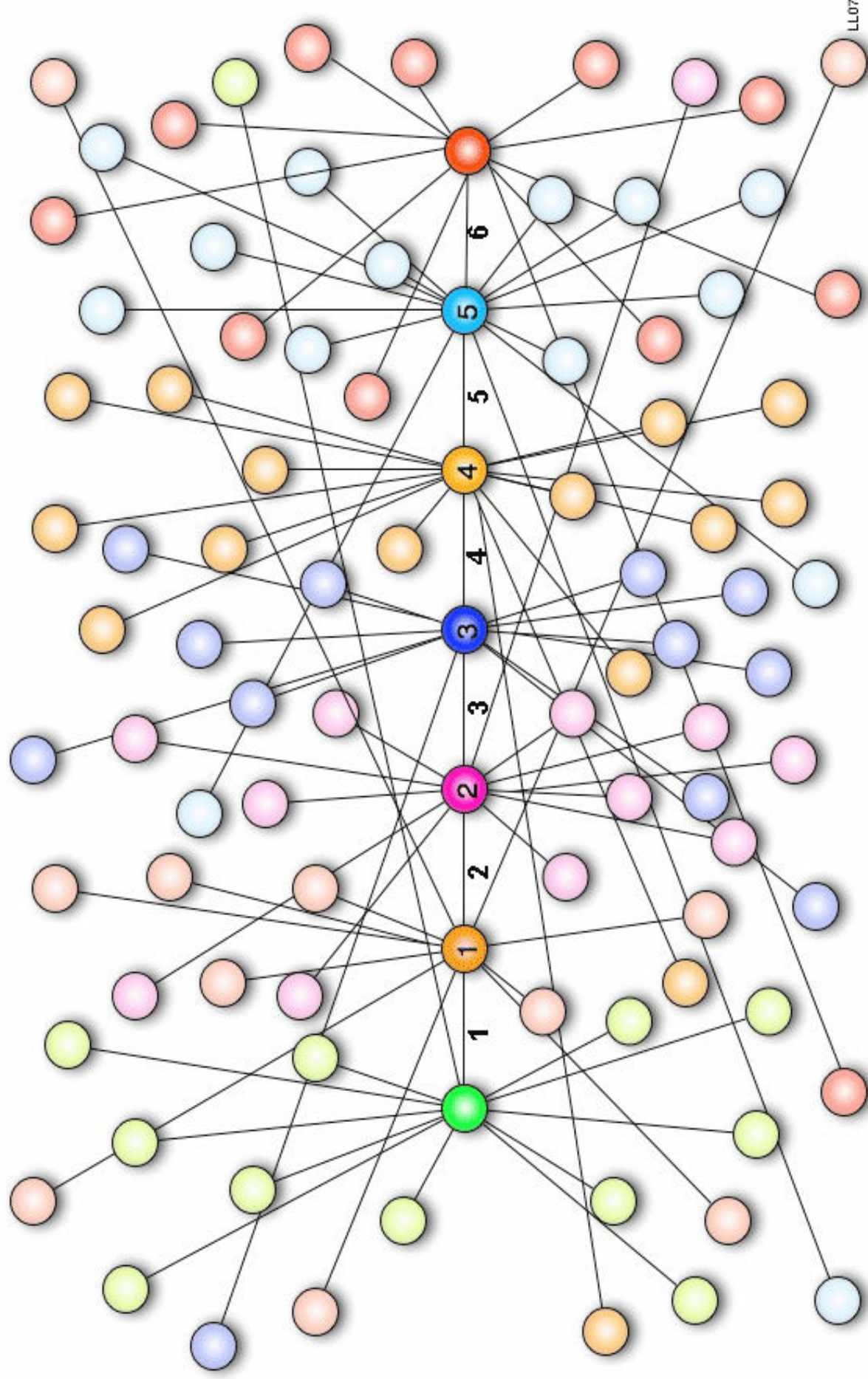
- ▶ L'environnement de l'entreprise est un système dynamique et entropique comme l'environnement informationnel dans lequel elle évolue
- ▶ L'IE et la veille stratégique ont pour but ultime la prévision ou la détection du « signal faible »
- ▶ Un signal faible est souvent une information sérendipitaire
- ▶ Détecter un signal faible c'est détecter le premier battement d'aile du papillon de la théorie du chaos Lorenz



La notion de chaos = jeu du
téléphone arabe =



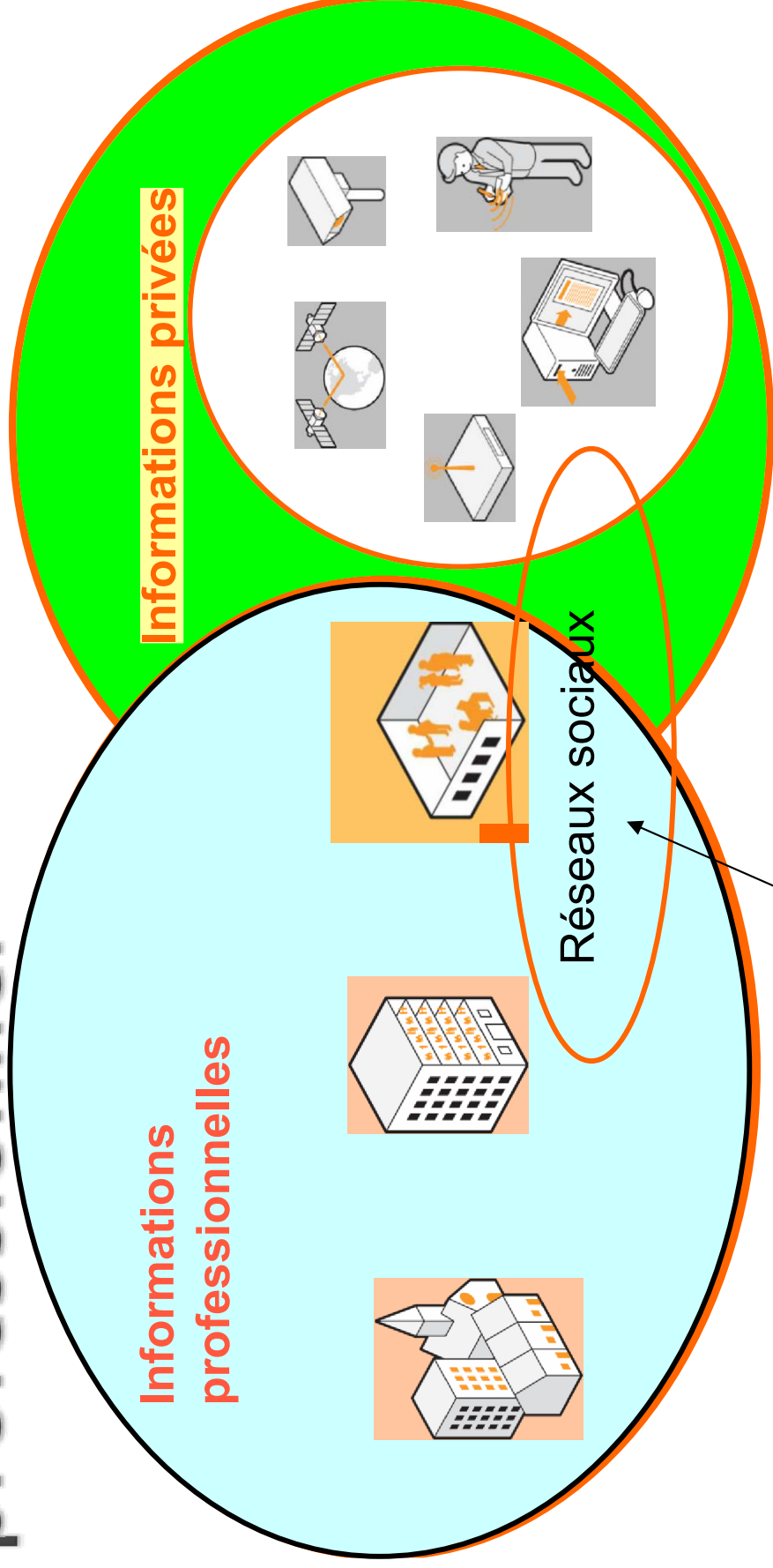
Le petit monde... des réseaux sociaux



Les risque 2.0



Les réseaux sociaux: la convergence du privé et du professionnel



L'information privée devient stratégique

Le syndrome du chasseur: le Web 2.0 et la protection de l'information

- ▶ Un veilleur est dans la position du chasseur (d'infos), mais sur le web 2.0, il est en même temps la proie
- ▶ Dans un processus de veille stratégique, l'une des facettes les plus importantes est la protection de l'information.
- ▶ Dans l'entreprise, toute information n'est peut-être pas stratégique, mais toute personne y travaillant détient de l'information dont la divulgation pourrait être préjudiciable

Prendre en compte la capacité de nuisance de l'internaute

- ❑ L'identité et de la réputation numérique dans l'entreprise devient un enjeu pour les employés et les responsables de ressources humaines (70 % de la valeur de l'entreprise)
- ❑ Une information négative publiée sur internet peut avoir de graves conséquences pour une entreprise qui devra gérer le déficit d'image ainsi engendré
 - Médiasance: encouragée par les jeux de masque du Net
 - Information préjudiciable lancée ou relayée de bonne foi (Un enfer pavé de bonnes intentions)
 - Volonté de nuire par dépit (la vengeance):
 - Action de déstabilisation orchestrée (formes de la *guerre économique*, qui relève aussi de la *guerre de l'information*)

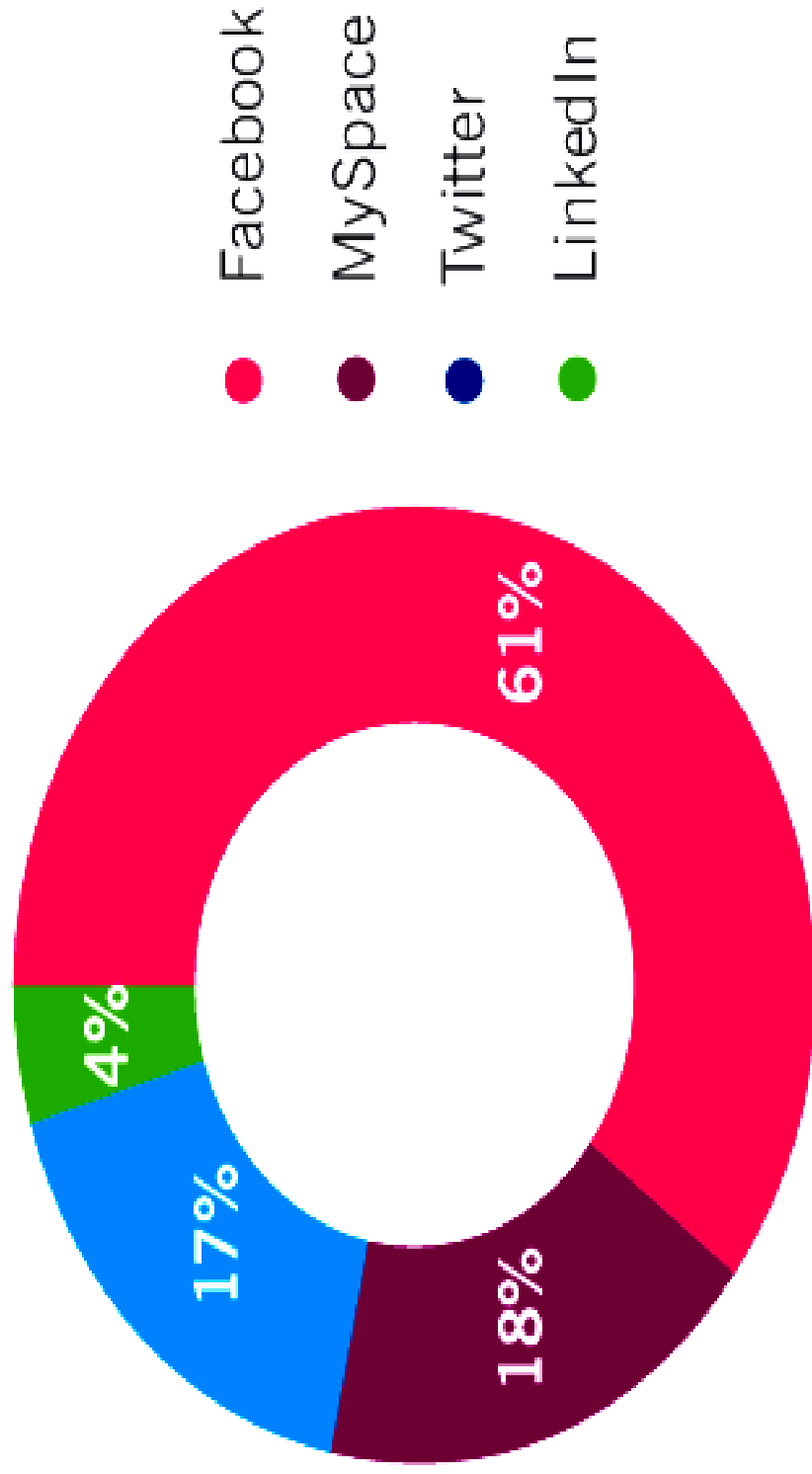
Les réseaux sociaux: Facebook

- ▶ Facebook: 400 millions d'individus interconnectés, (si c'était un état, il serait le quatrième le plus peuplé au monde
 - Chaque jour, 40 millions de messages
 - Chaque semaine, 2 milliards de liens vers des contenus externes y sont postés
 - Chaque mois, 2 milliards de photos sont téléchargées sur ce gigantesque annuaire
- ▶ Algérie: 818 500 utilisateurs dont un tiers de femmes (mai 2010)
- ▶ Quatrième plus gros site de l'internet: attire les mafias
 - Vol d'identité ou d'informations
 - Propagation de logiciels malveillants (Koobface)

Les réseaux sociaux: Facebook, Twitter...

- Facebook: plusieurs milliers d'applications, et très peu d'entre elles sont vérifiées (à l'inverse d'App Store d'Apple).
- Certaines appli sont volontairement malveillantes, d'autres présentent des failles de sécurité
- 9700 applications présentant de grosses failles de sécurité, y compris parmi les plus populaires.
- Selon ce même hacker 218 millions d'utilisateurs de Facebook ont été exposés en octobre à des applications présentant des failles de sécurité
 - Selon un hacker connu sous le pseudo de HarmonyGuy spécialiste de la sécurité sur les réseaux sociaux, sur son blog *theharmonyguy.com*

Selon Sophos Security Threat Report: 2010

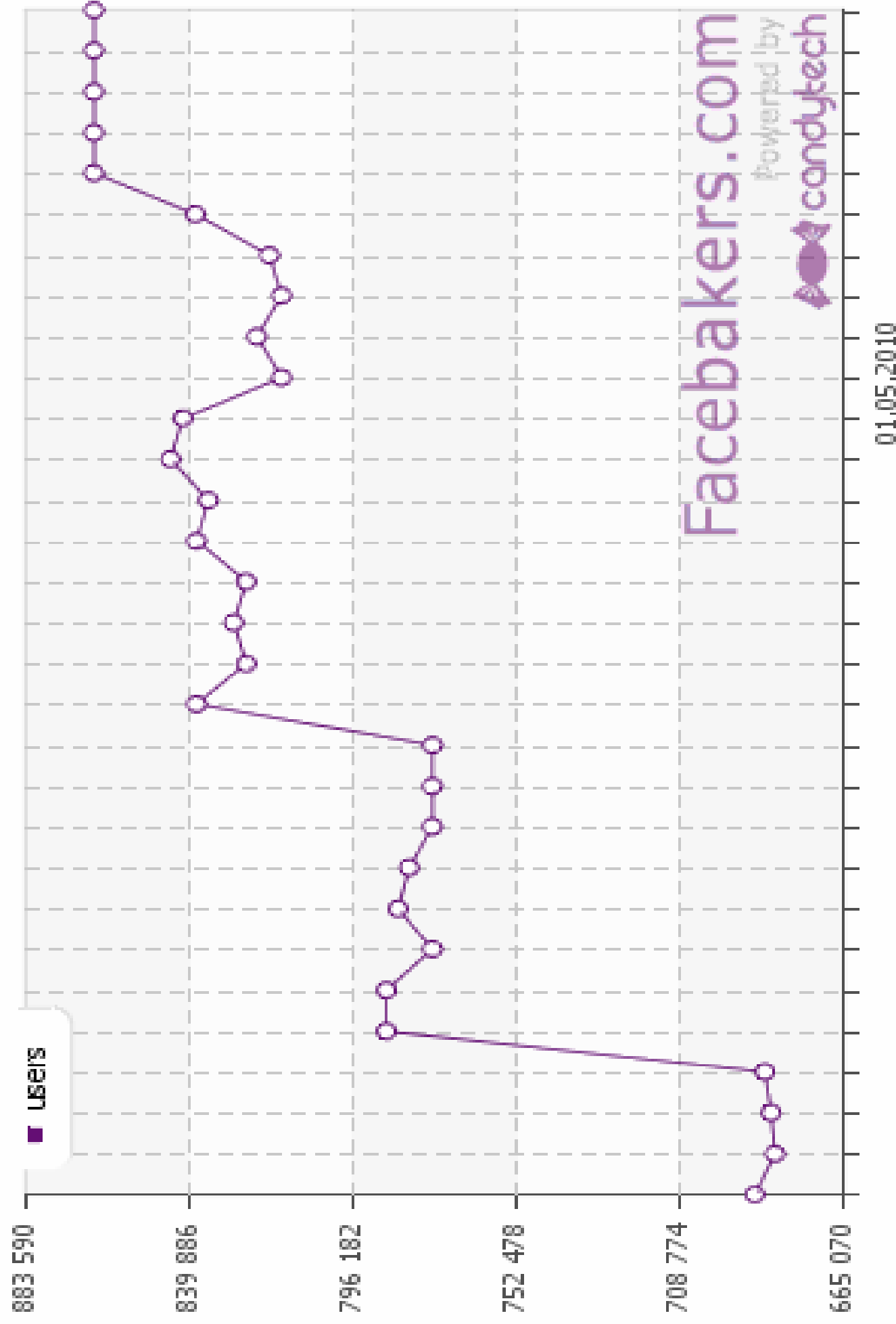


Which social network do you think poses the biggest risk to security?

Classement par pays des utilisateurs de Facebook (mai 2010)

- ▶ 1 United States: 118.688.120
- ▶ 2 United Kingdom: 24.594.380
- ▶ 3 Indonesia: 22.813.620
- ▶ 4 Turkey: 20.204.880
- ▶ 5 France: 17.329.700
- ▶ ...
- ▶ 43. Morocco (MA) 1.645.740
- ▶ 47. Tunisia (TN) 1.456.460
- ▶ 61. Algeria (DZ): 818.500 (le 16/05/2010 il y a 878660)

User Growth - Facebook Algeria

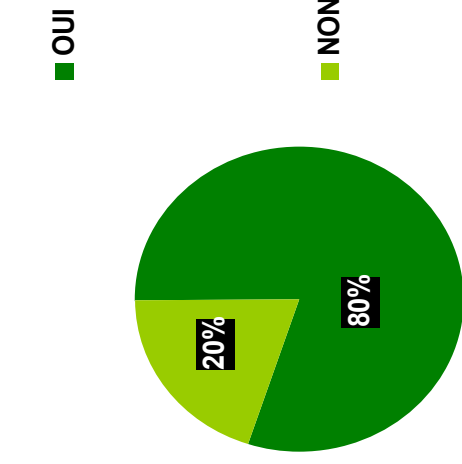


Les entreprises et les organisations face aux réseaux sociaux



Baromètre des stratégies RH et des réseaux sociaux: baromètre Novamétrie 2009

CONNAISSEZ-VOUS LE POURCENTAGE DE VOS COLLABORATEURS PRESENTS SUR DES RSN EXTERNES ?



PRESENCE SUR
RSN

« Oui, je fais partie moi-même de ces réseaux. »

VEILLE RH

« Oui, j'en ai connaissance, nous faisons de la veille
Rh sur ce sujet. »

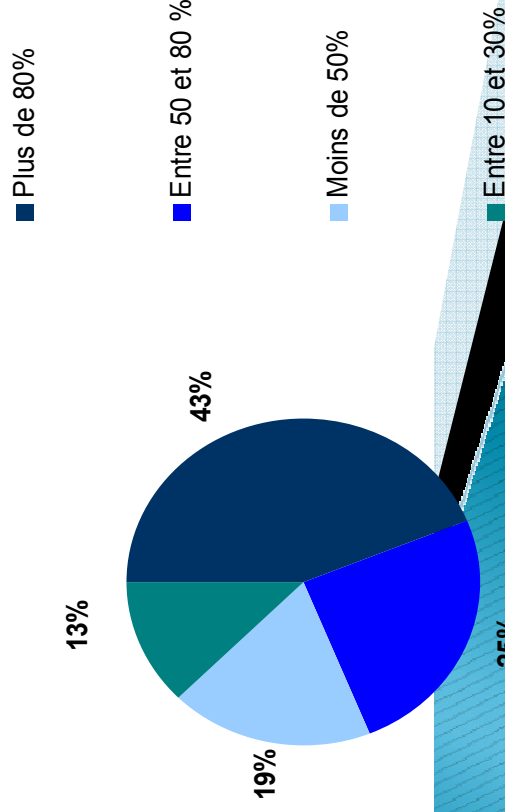
ABSENCE SUR
LES RSN

« Non c'est une information que je ne possède pas, je
n'appartiens à aucun réseau numérique. »

NON INTERESSE /
NON CONCERNE

« Non parce que ces informations ne m'intéressent pas
et ne me regardent pas. »

SI OUI, QUEL EST LE TAUX DE PRESENCE DE VOS COLLABORATEURS SUR LES RSN EXTERNES ?



« Nous sommes entre 80 et 100% sur des réseaux plutôt
personnels, on n'échange pas vraiment à titre professionnel, mais
on communique ou on se poste des photos, des vidéos. »

« C'est assez faible, moins de la moitié, la plupart de nos
collaborateurs ne sont pas nés avec ces outils, c'est une donnée
culturelle. »

L'EXISTENCE D'UNE CHARTE ?

COTE DRH

1/5 DES DRH ONT DÉJÀ ÉTABLI UNE CHARTE
D'UTILISATION DES RSN DANS LEUR ENTREPRISE

DES MESURES ALLANT DU RENFORCEMENT DE LA
CLAUDE DE CONFIDENTIALITÉ À L'INTERDICTION TOTALE
D'ACCÈS AUX RSN EXTERNES

1. RENFORCEMENT DE LA CLAUDE DE CONFIDENTIALITÉ CONTRACTUELLE
2. NOTE D'INFORMATION SUR LES NOUVELLES TECHNOLOGIES
3. UTILISATION RESTREINTE DANS LE TEMPS DE TRAVAIL
4. INTERDICTION D'ACCÈS

ENVIRON LA MOITIÉ DE CEUX QUI N'ONT RIEN FAIT
ESTIMENT QU'IL FAUT EN ÉTABLIR UNE

COTE COLLABORATEURS

POUR 86% DES COLLABORATEURS, IL N'EXISTE PAS UNE
CHARTÉ D'UTILISATION DES RSN DANS LEUR
ENTREPRISE

« Il n'y a rien qui est mis en place, évidemment c'est mal vu de les
utiliser trop souvent au bureau, un usage modéré devrait être tout
de même toléré. »

« Entre collaborateurs on peut converser via les réseaux externes,
c'est plus convivial, on utilise peu l'intranet pour se dire des choses
à titre personnel, c'est un mode parallèle de communication; pour le
côté strictement professionnel c'est l'intranet, et les informations
personnelles ce sont les réseaux externes. »

LES COLLABORATEURS FAVORABLES À UN CODE DE
BONNE CONDUITE

Comment les entreprises utilisent les pages « Fan de »

3 SUISSES

OBJECTIF Générer des commandes sur son site de commerce électronique à un coût maîtrisé.

CIBLE Femmes de 25 à 45 ans.
MOYENS Création d'une page « Fan de » animée par une salariée à plein-temps ; organisation de jeux-concours ; publicités sous forme de textes et d'images.

RÉSULTATS Objectif de vente atteint en moins de quinze jours.

CISCO

OBJECTIF Accompagner le lancement de la caméra compacte Flip et générer du trafic vers son site.

CIBLE Jeunes sportifs.
MOYENS Création d'une page « Fan de » ; organisation de jeux-concours ; placement de publicités sur une à deux semaines.

RÉSULTATS 190 000 clics en 24 heures vers Theflip.com ; 500 fans « très actifs » ambassadeurs de la marque.

CANON FRANCE

OBJECTIF Constituer une communauté autour de la marque et des produits, où seraient diffusés informations sur les lancements et conseils techniques.

CIBLE Population urbaine.

MOYENS Création d'une page « Fan de » et lancement d'une campagne ciblée « Devenir fan ».

RÉSULTATS Plus de 46 000 fans inscrits à ce jour. Publicité vue 31,8 millions de fois.

CAJOLINE

OBJECTIF Opération de fidélisation marque et produits.

CIBLE Femmes de 25 à 45 ans.

MOYENS Création d'une page « Fan de ».

Envoi de cadeaux à l'adresse physique des internautes.

RÉSULTATS : 50 000 fans en un mois ; plus de 70 000 cadeaux envoyés ; taux d'engagement (de clics) : 1,4 %, contre 0,15 % en moyenne sur Internet.

Challenges 15/04/2010

Greenpeace et Nestlé sur Facebook

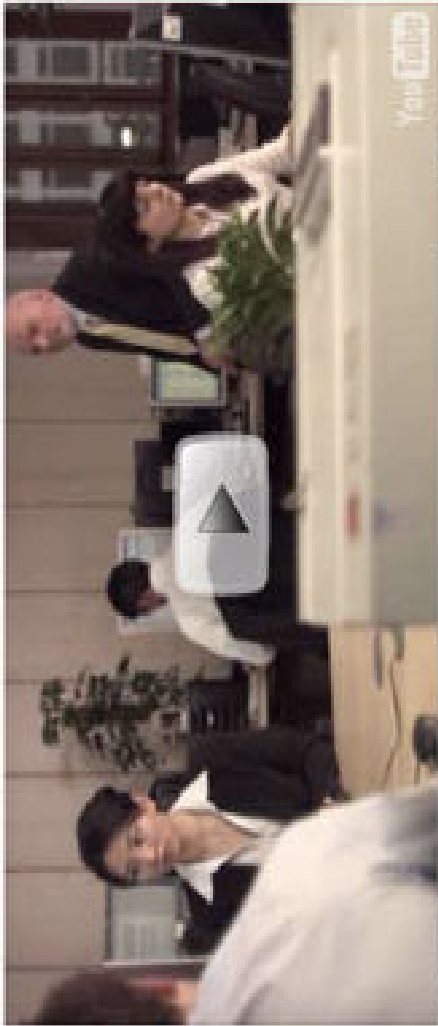
GREENPEACE

Killer

Ask Nestlé to give rainforests a break

SHARE THIS   

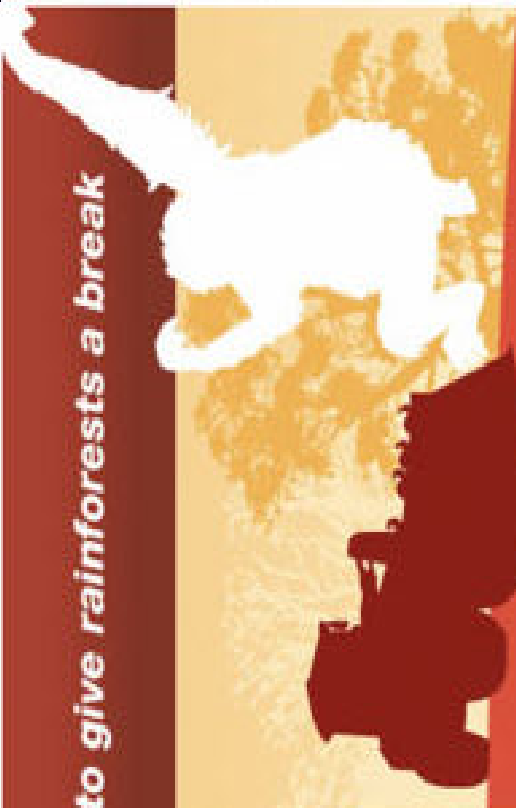
WATCH THE VIDEO



0:00 / 1:00   You Tube

NEED A BREAK? SO DOES THE RAINFOREST.

Nestlé, maker of Kit Kat, uses palm oil from companies that are



Greenpeace International Home | Get full story |
Your Kit Kat Campaigns! | Call Nestlé!

TAKE ACTION
SELECT YOUR REGION:

- ▶ Australia Pacific
- ▶ Austria
- ▶ Belgium (Dutch)
- ▶ Belgium (French)
- ▶ Israel
- ▶ Japan
- ▶ New Zealand

[Don't miss](#) [Facebook](#)

EthicsPoint

- ▶ Revendiquant 2 200 clients, ce cabinet entend aider les entreprises à « préserver leur réputation en identifiant les comportements susceptibles de contrevenir à leur code de conduite ». EthicsPoint met ainsi à leur disposition une hot line téléphonique et un site [Internet](#) sécurisés grâce auxquels les salariés peuvent rapporter une information de manière anonyme. Pour ce faire, le salarié d'une entreprise cliente d'EthicsPoint reçoit un code secret lui permettant de laisser un message sur le site [Ethicspoint.com](#). Le contenu de ces messages est alors transmis à l'entreprise cliente.
- ▶ à la tête de cette société un ancien haut gradé de l'armée américaine reconverti dans le business

Comment l'armée française gère les réseaux sociaux

- ▶ La grande muette n'a jamais interdit l'accès à internet, et aux réseaux sociaux en particulier, depuis les ordinateurs qu'elle met à disposition
- ▶ En revanche, les usages – à l'instar des autres moyens de communication (téléphone, fax, courrier postal) – sont soumis à un devoir de réserve et de discrétion prévu par l'article 4122-2 du Code de la défense
- ▶ Les militaires sont sensibilisés sur les usages de l'Internet. Des rappels sont régulièrement effectués et une plaquette d'information spécifique a été diffusée.
- ▶ La DGSIC (Direction Générale des Systèmes d'Information et de Communication) réfléchit même à l'opportunité de se doter d'un réseau social sur l'intranet du ministère de la Défense.

Le Pentagone face aux réseaux sociaux

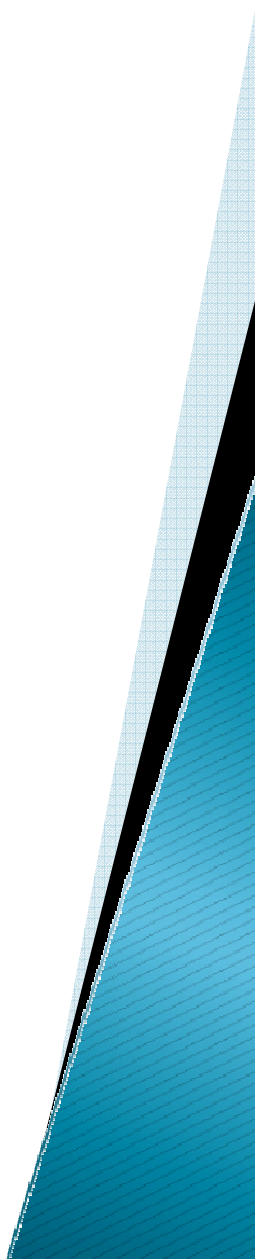
- Août 2009, le Pentagone ordonne une enquête interne sur l'usage des réseaux sociaux:
 - libéralisation sous conditions, l'accès depuis ses systèmes informatiques aux sites de réseautage
 - Tous les militaires sur le terrain, ainsi que dans les différents services, pourront accéder à Twitter, Facebook, MySpace, YouTube et autres blogs, « depuis des ordinateurs gouvernementaux non classifiés pour autant que cela ne compromette pas la sécurité opérationnelle ou n'implique des activités ou des sites prohibés » précise le communiqué du DoD
 - Concilier l'impératif de sécurité avec les opportunités qu'offrent les réseaux sociaux en termes de partage d'information et de prise de décision.
 - responsabilisation des utilisateurs qui recevront des formations adéquates
 - Les différents commandements de l'armée pourront si nécessaire retreindre les accès dans le cadre d'opérations sensibles
 - Responsabilisation des utilisateurs qui recevront des formations adéquates

Réactions face au web 2.0: les « federal trojan »

- ▶ « Magic Lantern: en 2001, le gouvernement américain a révélé avoir développé un trojan à des fins d'enquête pour le FBI: « Magic Lantern »
- ▶ La « Magic Lantern » est ce que l'on appelle un federal Trojan. Le terme "policeware" est également utilisé en référence aux "malwares".
- ▶ Depuis la Magic Lantern, le FBI a continué de développer le concept de Federal Trojan, notamment avec le logiciel CIPAV qui s'est rendu célèbre lors de l'affaire Timberlinebominfo
- ▶ Allemagne: l'utilisation d'un BundesTrojaner est légalement justifiable lorsque la protection de la Constitution ou la sécurité nationale est en jeu
- ▶ La Skype Capture Unit: En Allemagne, la société Digitask spécialisée dans la sécurité des télécommunications propose à l'état allemand d'utiliser un Trojan pour écouter les conversations Skype SSL
- ▶ L'Etat chinois diffuse une version buggée Skype
- ▶ Les gouvernements suédois et autrichien ont également annoncé qu'ils réfléchissaient à un cadre juridique pour des Trojans Fédéraux.

Suivi d'attaques par ingénierie sociale

- ▶ Piratage d'une entreprise via Facebook
- ▶ Le projet Gadyar
- ▶ Hacker Croll



Le hacking



Le Google hacking

The screenshot shows a Mozilla Firefox browser window with the address bar displaying the search query: `http://www.google.com/search?hl=fr&rl=&client=firefox-a&hs=6YN&rls=org.mozilla%3Afr%3Aofficial&channel=s&q=intitle%3Aindex.of+passwd&btnG=Re`. The search results for `intitle:index.of passwd` are displayed, showing approximately 146,000 results in 0.27 seconds. The results list several links, including:

- [Index of /etc/passwd](#) - [Traduire cette page]
- [master.passwd](#) 31-Jul-2003 12:55 9k [] msads.dll 31-Jul-2003 12:55 63k [TXT] ...
- [passwd.txt](#) 31-Jul-2003 12:55 1k [TXT] [passwd](#) 31-Jul-2003 12:55 1k [TXT] ...
- [gray-world.net/etc/passwd/](#) - Pages similaires
- [Facebook Mirror | Index of /cpan/modules/by-category...](#) - [Traduire cette page]
- [passwd-DB-1.03.tar.gz](#) 30-Jun-2006 16:34 3 8K [] [passwd-Linux-1.2.tar.gz](#) 10-Sep-2007 15:08 5.1K [TXT] [passwd-Samba-0.14.readme](#) 20-Mar-2008 06:46 2.3K [] ...
- [mirror.facebook.net/cpan/modules/by.../04.../passwd/](#) - En cache
- [Index of /passwd](#) - [Traduire cette page]
- [Index of /passwd](#). Name Last modified Size Description. [DIR] Parent Directory 14-Apr-2006 10:40 - [] [passwdlist.txt](#) 14-Apr-2006 10:44 1k [] ...
- [www.gialle.org/passwd/](#) - En cache - Pages similaires
- [intitle:index.of passwd](#) - [Traduire cette page]
- [intitle:index.of passwd](#) intitle:"Index of. etc" [passwd](#) intitle:index.of pwd.db [passwd](#) intitle:index.of ws.ftp.ini intitle:index.of people.lst ...
- [hacking.feedfury.com/.../15618076-intitle-index-of-passwd.html](#) - En cache - Pages similaires
- [Index of /password](#) - [Traduire cette page]
- [... 23:49 1k inyongo.asp](#) 18-Apr-2004 23:49 1k [pasadena.html](#) 18-Apr-2004 23:49 8k
- [password.asp](#) 18-Apr-2004 23:49 1k [passwords.txt](#) 18-Apr-2004 23:49 1k.
- [eorr.home.net/corn/passwd/](#) - En cache - Pages similaires
- [Index of /etc/passwd](#) - [Traduire cette page]
- [mailform.pl](#) 31-Jul-2003 12:55 4k [TXT] [mailto.cgi](#) 31-Jul-2003 12:55 2k [TXT] [master.passwd](#) 31-Jul-2003 12:55 9k [] [msads.dll](#) 31-Jul-2003 12:55 63k [TXT] ...
- [lineman.net/etc/passwd/](#) - En cache - Pages similaires
- [Index of /passwd](#) - [Traduire cette page]

The browser interface includes a search bar, navigation buttons, and a sidebar with links like 'Web', 'Images', 'Videos', etc.

[All Sites](#)[About](#)[Develoners](#)[Open Source](#)[Careers](#)

[Index of /cpan/modules/by-category](#)

[/04 Operating System Interfaces/Passwd](#)

Name	Last modified	Size
 Parent Directory	-	-
 EESTABROO/	23-Aug-2009 12:22	-
 STRZELEC/	07-Apr-2010 12:48	-
 Passwd-DB-1.01.tar.gz	08-Apr-1999 09:21	3.5K
 Passwd-DB-1.03.tar.gz	30-Jun-2008 16:34	3.8K
 Passwd-Linux-1.2.tar.gz	10-Sep-2007 15:08	5.1K
 Passwd-Samba-0.14.readme	20-Mar-2008 06:46	2.3K
 Passwd-Samba-0.14.tar.gz	20-Mar-2008 12:27	3.0K
 Passwd-Solaris-1.2.tar.gz	10-Sep-2007 15:21	5.0K
 Passwd-Unix-0.51.readme	11-May-2009 04:02	8.0K
 Passwd-Unix-0.51.tar.gz	11-May-2009 02:04	11K
 Passwd-Unix-0.52.readme	11-May-2009 04:02	8.0K
 Passwd-Unix-0.52.tar.gz	02-Aug-2009 06:16	11K

Démocratisation et vulgarisation du hacking

- ▶ Requêtes hacking des réseaux sociaux
 - Hacking Facebook: 29 500 000 de résultats
 - Hacking Twitter: 25 700 000 résultats
 - Hacking Myspace: 8 510 000 résultats
 - Hacking LinkedIn: 4 390 000 résultats
 - Hacking Viadeo: 41 000 résultats
 - « google hacking » : 280 000 résultats
- ▶ Conficker apparu fin 2008 est à comparer au virus du SIDA
 - il désactive toutes les défenses, ce qui permet aux autres virus d'entrer plus facilement)
 - se met à jour automatiquement, tout en empêchant les mises à jour de l'ordinateur

L'Algérie est sous la menace du piratage informatique

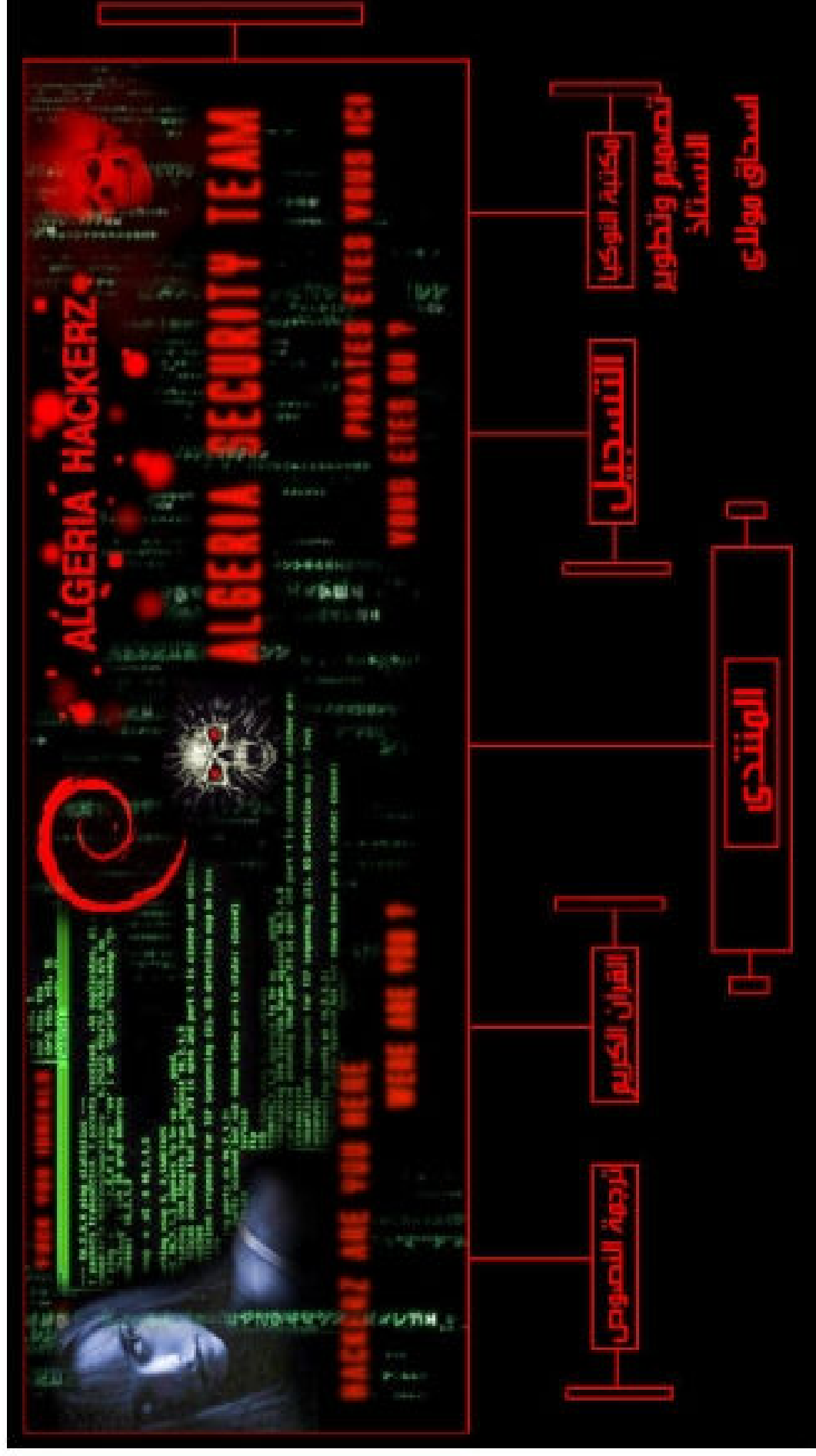
- ▶ Mise en place par l'Algérie à l'Institut national de la police criminelle, à Saoula d'une formation qui tente de répondre problématique du piratage destinée aux cadres de la Sûreté nationale.
- ▶ Pour la DGSN, cette formation, vise notamment à l'issue du cursus à procéder à la constitution, au niveau de chaque sûreté de wilaya, de cellules chargées de la lutte contre la cybercriminalité.
- ▶ Contenu de la formation:
 - Fonctionnement de l'internet
 - Investigation dans le domaine de l'informatique
 - Techniques d'identification et problématique des traces numériques
 - aspects juridique de la cybercriminalité,
 - Sécurité des réseaux...

Utilisation de logiciels piratés: risque de logiciels infectés

TABLE 1: Top 25 High and Low Piracy Rates

HIGHEST PIRACY		LOWEST PIRACY	
Georgia	95%	United States	20%
Bangladesh	92%	Japan	21%
Armenia	92%	Luxembourg	21%
Zimbabwe	92%	New Zealand	22%
Sri Lanka	90%	Austria	24%
Azerbaijan	90%	Belgium	25%
Moldova	90%	Denmark	25%
Yemen	89%	Sweden	25%
Libya	87%	Switzerland	25%
Pakistan	86%	Australia	26%
Venezuela	86%	Finland	26%
Indonesia	85%	Germany	27%
Vietnam	85%	United Kingdom	27%
Iraq	85%	Netherlands	28%
Ukraine	84%	Norway	28%
Algeria	84%	Israel	32%
Montenegro	83%	Canada	32%
Paraguay	83%	Ireland	34%
Cameroon	83%	South Africa	35%
Nigeria	83%	Singapore	36%
Zambia	82%	UAE	36%
Bolivia	81%	Czech Republic	38%
Guatemala	81%	Taiwan	39%
China	80%	Reunion	40%
El Salvador	80%	France	41%

Le « hacktivism »



Les « hacktivismes »

Hacked by ishak

تم اختراقه من طرف اسحاق

xd_10@hotmail.fr

www.kais-dz.com

Usage frauduleux des documents papiers



Usage frauduleux des documents papiers

- ▶ Selon l'enquête du [Credoc](#) auprès des ménages et des entreprises franciliennes
 - 90% des établissements d'Ile-de-France, considèrent que les risques d'usurpation d'identité ou d'espionnage sont nuls ou peu élevés
 - Plus de 2/3 des établissements estiment qu'il est peu probable de trouver des données confidentielles dans leurs déchets
 - 84% des établissements n'ont pas engagé d'actions contre les risques d'espionnage économiques
 - 90% des établissements n'ont donné aucune indication (aux salariés) en ce qui concerne la destruction des données stratégiques
 - 58% des établissements jettent leurs documents sans les détruire
 - Plus la moitié contenait des documents financiers
 - 13% contenait des documents contenant toutes les données permettent d'usurper une identité

Les ménages

- ▶ (Seuls) 43% des franciliens cherchent à se prémunir contre les risques d'usurpation d'identité
- ▶ 9% jettent des papiers sans les déchirer
- ▶ Chez 20% des ménages, les poubelles contenaient des données bancaires
- ▶ Le risque existe chez 2/3 des PME, et 1/5 des ménages étudiés

Protection et défense du patrimoine informationnel

Mettre en place un gestionnaire de communauté (community manager)

- ▶ Les missions du Community Manager
 - Rappeler les règles de bonne communication
 - Organiser, favoriser l'échange d'expériences au sein de la communauté et améliorer sa cohésion
 - Développer la visibilité d'une marque au sein de communautés sur le web
 - Améliorer la plate-forme technique de la communauté
- ▶ Compétences requises
 - Capacité à organiser des événements réunissant la communauté.
 - Capacité à mobiliser des acteurs (entreprises, collectivités, associations) et à créer des partenariats
 - Connaissance des techniques de veille et de recherche d'information.
 - Connaissance métier sur les thématiques qui fédèrent la communauté.
 - Connaissance pratique des réseaux sociaux et communautaires tels que Youtube, LinkedIn, Ning, Viadeo, Facebook, Twitter, la blogosphère et les forums.

Mettre en place un gestionnaire de communauté (community manager)

2

- ▶ Formation: pas de formation diplômante spécialisée actuellement en France. L'Apec donne cependant les formations les plus recherchées pour ce profil:
 - Formation universitaire supérieure Bac + 2 à Bac + 5 en sciences humaines ou écoles de commerce, complétée par une spécialisation dans la communication on-line.
 - Ecoles spécialisées en communication, marketing, journalisme, ou relations publiques
 - A L'institut Léonard de Vinci, il existe deux MBA MCI qui proposent une large place au métier de community manager
- ▶ Rattachement hiérarchique
 - Responsable d'intelligence économique
 - Responsable de la communication
 - Directeur de la communication
 - Directeur marketing

Mise en place d'une veille sécurité

- ▶ Établissement d'un cahier des charges des logiciels et technologies à suivre:
 - Technologies web: Apache, Domino, Websphere...
 - Système d'exploitation: Windows, Linux, Solaris...
 - Logiciels et serveurs d'entreprise: Outlook, Exchange, Lotus, Internet Explorer, SAP...
 - Les bases de données: Oracle, MySql, Sybase, Informix...
 - Les équipements d'infrastructures: Antivirus, Firewall, VPN...
 - Les équipement mobiles: téléphone 3G, PDA, Blackberry...
- ▶ Surveillance des apparitions des vulnérabilités et des correctifs: les virus les plus dangereux arrivent par les failles non corrigées dans les systèmes
- ▶ Suivi des techniques d'attaques informatiques

Mise en place une veille RH

- ▶ L'environnement externe et la concurrence
 - Ethique flexible
- ▶ Sa propre entreprise
 - Personnel
 - Dirigeants/ responsables
 - Représentants du personnel (syndicalistes, membres du comité d'entreprise, délégués...)
 - Fournisseurs principaux
 - Clients principaux
 - Autres postes stratégiques (négociateurs, R&D, commerciaux...)

Predictibilité des actions:

« *Minority report* »

- ▶ Le département de la justice des mineurs de Floride utilise depuis la mi-avril un logiciel d'analyse prédictive, qui estime les chances de récidives d'un délinquant et suggère des solutions de placement ou d'orientation.
- ▶ Selon IBM, ce logiciel, nommé Predictive Analytics, peut donner aux gouvernements du monde entier un « moyen pour créer des communautés plus sûres via l'identification, la prévision, l'intervention et la prévention des activités criminelles »

Imaginons un trojan informatique qui commanderait l'esprit humain

- ▶ En 2009 des chercheurs ont mis au point une technologie qui permet à la pensée d'agir directement sur un ordinateur ou de manœuvrer une chaise roulante.
- ▶ Comment protéger l'humanité d'un dispositif cybernétique qui permettrait d'interférer avec le fonctionnement des cerveaux ?

Merci de votre ...patience